Intel® Active System Console v6.0

User Guide

July 2013

Legal Statements

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS FOR THE PURPOSE OF SUPPORTING INTEL DEVELOPED SERVER BOARDS AND SYSTEMS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Intel is a trademark of Intel Corporation in the U.S. and other countries.

Microsoft, Windows, Windows Server, Active Directory, and Vista are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.

* Other names and brands may be claimed as the property of others.

Copyright © 2008 – 2013 Intel Corporation. All rights reserved.

Revision History

Description	Revision Date
Support for Intel® Xeon® Processor E3-1200 v3 family based Platforms	April 2013
Support for Intel® Xeon® Processor E5 family based Platforms	July 2013

Contents

Legal Statements 2

Contents 4

1 Introduction 7

1.1 Target Audience 7
1.2 Overview 7
1.3 Features and Benefits 9
1.4 System Requirements 10
1.4.1 Supported Operating Systems 10
1.4.2 Browser Requirements 10
1.4.3 Supported Platforms 11
1.5 Supported Languages 11
1.6 Additional Information 11
1.6.1 Third Party Source Code/Binaries 11
1.6.2 Support Information 11
1.6.3 Related Documentation 12
1.7 Terminology 12

2 Getting Started 14

2.1 Installing Intel® Active System Console 14
2.2 TCP Information 15
2.3 Uninstalling Intel® Active System Console 16

3 Navigating Intel® Active System Console 17

3.1 System Information 19
3.1.1 Viewing System Health 19
3.1.2 Viewing System Summary 20
3.1.3 Viewing Processor Summary Readings 21
3.1.4 Viewing Memory Device Readings 21
3.1.5 Viewing Temperature and Fan Readings (Cooling Sensors) 22
3.1.6 Viewing Voltage and Current Sensors Readings 23
3.1.7 Viewing Chassis Information 23
3.1.8 Viewing Storage Readings 24
3.1.9 Viewing Miscellaneous Readings 25
3.1.10 Viewing System Events 25

4 Configuring Server Hardware and Reports Generation 27

4.1 Configuring BMC 27
4.1.1 Configuring BMC Users 27
4.1.2 Configuring Network 29
4.1.3 Configuring Serial Over Lan (SOL) Settings 30
4.1.4 Configuring SNMP Alerts 31
4.1.5 Configuring BIOS 31

4.1.6 Configuring Intel® Dynamic Power Node Manager (Node Manager) 32
4.1.7 Configuring Basic Email: Use Default Email Profile 34
4.1.8 Configuring Advanced Email: Create and Apply Email Profiles 35
4.2 Generating Reports 36
4.3 User Settings..... 36
4.4 Viewing Software Updates..... 37
5 Security Features 38
5.1 Security Recommendations 40
6 Troubleshooting Guidelines.....41

<**This page is intentionally left blank.**>

1 Introduction

The Intel® Active System Console is a simple, lightweight web application console that gives you a dashboard view of the Server hardware on which it is running. It helps you proactively monitor the health of your Server, allows remote configuration of Server, tracking of assets, alerting of any issues and generation of asset reports.

The Intel® Active System Console is a product offering from the Intel® System Management Software - a suite of software products designed to reduce the cost and time of managing servers and keep businesses running 24/7.

IASC is included with almost all Intel® Server Products at no additional charge giving your customer "peace of mind" that servers are healthy.

IASC offers the following:

- **Proactive alerting** allows the server administrator to plan routine maintenance activities and avoid unplanned downtime
- **Asset Inventory** tells you what components are installed in the server without having to shut down and open the system
- **Remote debug** isolates problems quickly saving hours and even days in the time it takes to debug and fix the issue.

1.1Target Audience

The purpose of this document is to help system/server administrators install and use the Intel® Active System Console. It provides you detailed information on the features and benefits of Intel® Active System Console and how to use them. It describes the software requirements, supported operating systems, and the supported platforms. It also explains the installation and un-installation process.

1.2Overview

The Intel® Active System Console helps you in proactive monitoring of the health of your Server, allows remote configuration of Server, tracking of assets, alerting of any issues and generation of asset reports. It gives you an overall view of the server hardware. This comprises information on hardware components of the system - overall health of the server and component health, sensors, System Event Log (SOL), storage (Logical Drives, Hard Drives), processors, memory, Field Replaceable Unit(FRU)s as well as BMC configuration.

Get Peace of Mind

It improves security, reduces costs, and helps businesses move from reactive to proactive system management. The software enables secure remote management and monitoring of servers, clients, and applications from virtually any location—in a way that IT generalists can understand without attending weeks of training. It's all about IT made easy:

Simple

- Makes it easy to set up and maintain a reliable and secure IT infrastructure
- Streamlines tasks throughout server life cycle with remote management
- Manages IT functions with a single suite of tools

Secure

- Keeps IT informed with automated daily health reports and alerts
- Improves reliability and stability with application and patch deployment

Smart

- Designed specifically for small to midsize business
- Reduces travel time and costs
- Provides a proactive solution to server management with reports and alerts

IASC displays the hardware sensors, Field Replaceable Unit (FRU) data, and System Event Log (SEL) for any system.

To launch the Intel® Active System Console, go to **Start> Programs**> **Intel® Server Management Software >Intel® Active System Console**.

You can also launch IASC from any client using the URL:
https://<ipadddressofserver>:9393/asc

1.3Features and Benefits

This section discusses the features and benefits of Intel® System Management Software suite of Products in general and the IASC in particular.

Intel® System Management Software

The following table lists the comparative features and benefits of Intel® System Management Software suite of Products:

Features	Intel® Active System Console	Intel® SNMP-SA
Server Environment	1-10 servers	Enterprise
User Interface	Web Based	Integrates into enterprise tools such as HP* OpenView
Operating System Support	Windows, Linux	Windows, Linux
Single, easy to use console	X	
Hardware Predictive Failure Analysis	X	X
Sensor readings	X	X
Hardware Event Log	X	
Hardware and Software Inventory	X (Hardware and Operating System)	
OS and Application Monitoring		
Software Patch Deployment		
Application Deployment		
Alerting	X (Email and BMC SNMP)	X (SNMP)
Reporting	X	
BMC Configuration	X	
Power Management	X	
Performance Views		
Remote Management	X	X
Multi Server Management		
Remote Power On/Off/Reboot		
Serial Over LAN (Console Redirection)		
OEM Customization	X	

Intel® Active System Console

The Intel® Active System Console has the following features:

- Viewing System Health in the Dashboard
- Viewing Other System Information as follows:
  - Viewing System Summary
  - Viewing Processor Summary Readings
  - Viewing Memory Device Readings
  - Viewing Temperature and Fan Readings (Cooling Sensors)
  - Viewing Voltage and Current Sensors Readings
  - Viewing Chassis Information
  - Viewing Storage Readings
  - Viewing Miscellaneous Readings
  - Viewing System Events
- Generating Reports
- Checking for software updates

1.4System Requirements

This section details the software requirements, supported operating systems and the supported platforms for the Intel® Active System Console.

1.4.1 Supported Operating Systems

- Microsoft Windows* Server 2012
- Microsoft Windows* Server 2008 R2 SP1
- Red Hat* Linux* Enterprise 5.9 (x86/x64)
- Red Hat* Linux* Enterprise 6.4 (x86/x64)
- SuSE* Linux Enterprise Server 10 SP4 (x86/x64)
- SuSE* Linux Enterprise Server 11 SP2 (x86/x64)

1.4.2 Browser Requirements

The application has been tested to run on Microsoft* Internet Explorer 7.x or later and Mozilla Firefox* 3.6 or later versions. It is best viewed in screen resolution from 1024 X 768 to 1440 X 900.

1.4.3 Supported Platforms

- Multi-Core Intel® Xeon® Processor E3-1200 V3 Sequence-based Servers
- Multi-Core Intel® Xeon® Processor E5 Sequence-based Servers

For the latest and up-to-date list of supported operating systems, system requirements and platforms supported refer to the release notes available with the product.

1.5Supported Languages

English only.

1.6Additional Information

This section lists additional IASC related information that will help you use it appropriately.

1.6.1 Third Party Source Code/Binaries

Link to third party source code/binaries:
http://support.intel.com/support/motherboards/server/sysmgmt/sb/CS-031025.htm

1.6.2 Support Information

If you encounter an issue with your server platform or management software, please follow these steps to obtain support on your product.

1. Get connected to our support web page for 24x7 support when you need it to get the latest and most complete technical support information on all Intel® Enterprise Server, Storage Platforms and Management Software. Information available at the support site includes:

- Latest BIOS, firmware, drivers and utilities available through Intel's download center.
- Product documentation and flash demos, installation and quick start guides
- Full product specifications, technical advisories and errata
- Compatibility documentation for memory, hardware add-in cards, chassis support matrix, and operating systems
- Server and chassis accessory parts list for ordering upgrades or spare parts
- A searchable knowledgebase to search for product information throughout the support site

2. Utilize the community forums or chat with a live person.

3. You can also contact an Intel support representative using one of the following support phone numbers. Charges may apply. Intel customer support suggests running the Intel® System Information Tool (depending on the operating system being used) for Microsoft Windows*, Linux* or EFI* to extract relevant data that pertains to the issue being encountered and provide the information when asked by a support agent.

Intel now offers Channel Program members round-the-clock 24x7 technical phone support on Intel® server boards, server chassis, server RAID controller cards, and Intel® Server Management.

Warranty Information

Connect to Intel's website to obtain warranty information.

NOTE: Requires Login to the Reseller Site to obtain the 24x7 Number.

1.6.3 Related Documentation

The following table lists the related documentation:

Document/ Information	Source
Intel® Active system Console Release Notes	Available at the same package

1.7Terminology

The following table lists the terminology used in this document and the description:

Term	Description
BMC	Baseboard Management Controller
CIM	DMTFs Common Information Model - CIM provides a common definition of management information for systems, networks, applications and services, and allows for vendor extensions
GUI	Graphical User Interface
Intel® SMS	Intel® System Management Software
IPMI	Intelligent Platform Management Interface. Operates independent of the operating system (OS) and allows you to manage a system remotely even in the absence of the OS
RMCP	Remote Management Control Protocol – Protocol used by IPMI for communicating over LAN
SEL	System Event Log
SMBIOS	System Management BIOS (SMBIOS) is specification to lay out data structures (and access methods) in a BIOS which allows a user or application to store and retrieve information specifically about the Server
SNMP	Simple Network Management Protocol
SOL	Serial Over LAN

Term	Description
Upgrade	Enhanced versions of Intel® SMS with new platform support or new features are uploaded to Intel Website. Users installing Intel® SMS from a CD can upgrade to a new version using multiple ways. Intel recommends all users to upgrade to a new versions

2 Getting Started

This section provides information on how to install and use the Intel® Active System Console.

2.1 Installing Intel® Active System Console

For Linux*

To install the software, run with root privilege.

- If you downloaded the tar file, run the following command to unzip the package

  ```
  tar  -xvf  [ASC package name]
  ```

- If you are using CD/DVD to install, then browse to ...

  Then run the following commands.

  ```
  *cd ASC
  *./install
  ```

  The script auto-detects OS and Version (RHEL/SLES)

For Microsoft Windows*

- Insert Intel® Server Deployment and Management media, go to System Management Software Tab or user can browse ASC package folder and start the ASC installation main interface manually.

- Click on the "Click to Install" button for Intel® Active System Console Install. This will take you to the prerequisite Page, choose "Install Software" if enabled. Then, once the prerequisite software is installed click the "Continue Installation" button.

***Notes**:*

- *While installing, user will be asked to change the default password of "admin".*

  *We recommend you set a strong password for "admin" (for example, use a combination of letters, numbers, or keyboard characters not defined as letters or numerals such as ` - _ = + ! ~ # @ $ * : ; . , ? & ^)*

- *The IASC installed in the server also serves as an MSM agent monitoring this server.*

2.2 TCP Information

The following TCP ports are used by Intel® Active System Console.

Port #	Description	Firewall Exception Required
7777	Use for discovery and management by Intel® Multi Server Manager (MSM).	Yes **
9393	Use for web server hosting	Yes ***
4369	Use for socket based IPC on the software backend.	No
9191	Use for lighttpd web service.	No
521	Use for lighttpd web service / PHP CGI.	No

Notes:

** 7777 is required to add on the firewall approval list only when used to manage IASC with Intel® Multi-Server Manager.

*** 9393 is required to add on the firewall approval list if accessing IASC remotely over the network with a supported web browser.

Refer to **Chapter 5** for more security features.

2.3 Uninstalling Intel® Active System Console

To uninstall, run the following:

Linux* -
`cd /usr/local/asc/bin/`

`"sh uninstall"`

Windows* - You can uninstall ASC from Windows either

- from Add/Remove Program options
- from Start Menu->All Programs->Intel->Uninstall Intel® Active System Console

You will be asked to reboot the server to complete installation. You can either reboot immediately or postpone it. All files and registry entries will be completely removed only on reboot.

***Note**: The database will also be removed on uninstallation. If you want the database for any further storage make sure you copy the database SMS.db to appropriate location before uninstall.*

- *`/usr/local/asc/bin/SMS.db` (in Linux*)*
- *`C:\Program Files\Intel\ASC\SMS.db` (in Windows* 32 bit)*
- *`C:\Program Files (x86)\Intel\ASC\SMS.db` (in Windows* 64 bit)*

3 Navigating Intel® Active System Console

This section details how you can navigate the Intel® Active System Console to use its features.

By default, the Intel® Active System Console opens in the **System>Dashboard** view displaying overall server health as shown in Figure 1.

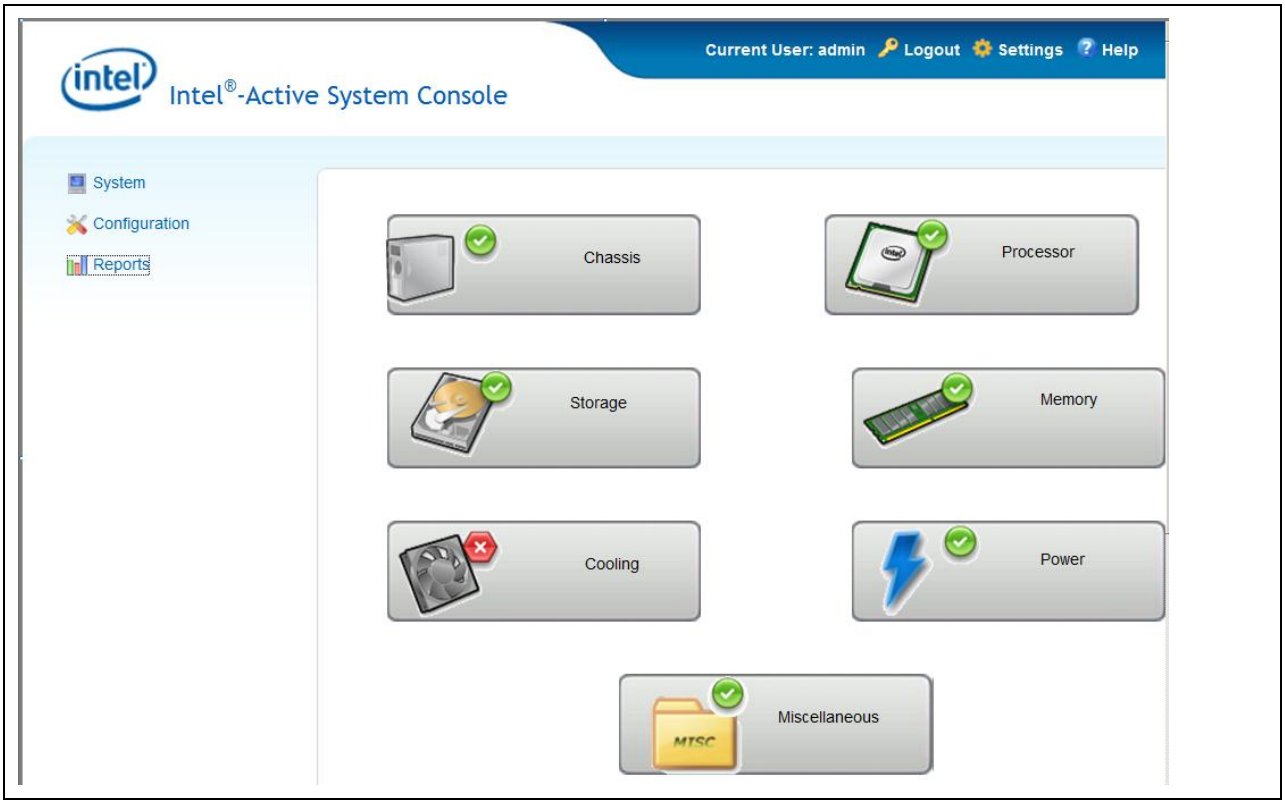


Figure 1. Intel ® Active System Console Login page (By default, IASC opens in Dashboard page)

The left side Navigation menu comprises buttons that have submenu items.

For a quick overview of the tasks performed by these buttons and their sub menu items see following Table:

Menu Button	Submenu	Task
System		
	Dashboard	Displays aggregate of the system health in the Dashboard (chassis, storage, cooling, processor, memory, and power).
	Summary	Displays a table of all hardware sensors and the threshold settings.
	Processor	Displays processor details and speed information.
	Memory	Displays memory size and type information.
	Cooling	Displays all System/Processor fans. It shows the current health status of the fan and the current reading of the fan in RPM.
	Power	Displays all Voltage and Current sensors. It shows the current health status and the current reading of the Voltage and Current sensors.
	Chassis	Displays the state of the chassis intrusion sensor and enables identifying the system by turning on/off the Chassis ID LED
	Storage	Displays information about the hard disk drives, logical disk drives, and media or DVD drives.
	Miscellaneous	Lists out all the Sensors which are not categorized under any of the main sensors. These include some BIOS and other discrete sensors.
	Events	Lists all the server event logs.
Configuration		
BMC	Baseboard Management Controller. Has the following submenu buttons: Manages the interface between system management software and platform hardware.	
	Users	Helps you add/delete/edit a BMC User.
	Network	Lists all the Network present on the motherboard.
	Serial Over Lan	SOL. Settings help change the Baud rate of the system.
	SNMP Alerts	Help send SNMP based alerts to the target server (fan failure, memory error, etc.
	BIOS	BIOS settings.
	Node Manager	Intel® Dynamic Power Node Manager. An advanced feature that helps set power policies resulting in

		saving system power.
Basic Email		Simple mail configuration that sends all server alerts to mail server.
Advanced Email		Helps configure user specific Email alerts. Feature-rich customized user settings available.
Reports		
Generation		Helps generate reports on many categories. For example, Asset Information, All System Events, Critical Events, Sensor Values ,and BMC Settings. The file can be exported either in XML, HTML, or CSV format.

3.1 System Information

This section lists the Hardware choices available shown in Figure 1.

The Hardware choices and their functions are listed in the following Table:

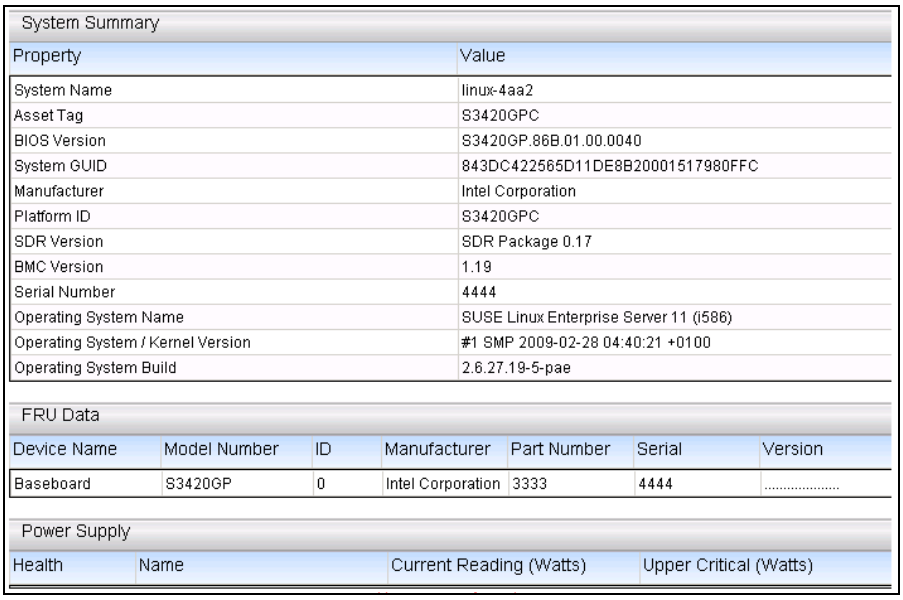
Hardware choice	Function
System - Displays system health information.	
Dashboard	Default IASC view. Displays chassis, Processor, Storage, Memory, Cooling, Power, and other Miscellaneous information in a convenient dashboard view.
Summary	Displays a table of all hardware sensors and the threshold settings.
Processor	Displays processor details and speed information.
Memory	Displays memory size and type information.
Cooling	Displays all System/Processor fans. It shows the current health status of the fan and the current reading of the fan in RPM.
Power	Displays all Voltage and Current sensors. It shows the current health status and the current reading of the Voltage and Current sensors.
Chassis	Displays the state of the chassis intrusion sensor and enables identifying the system by turning on/off the Chassis ID LED.
Storage	Displays information about the hard disk drives, logical disk drives, and media or DVD drives.
Miscellaneous	Lists out all the Sensors which are not categorized under any of the main sensors. These include some BIOS and other discrete sensors
Events	Lists all the server event logs.

3.1.1 Viewing System Health

The **System** page as shown in Figure 1 displays the health of the system and its components. The UI gets refreshed every 10 minutes.

3.1.2 Viewing System Summary

To view information on the board, BIOS, and Firmware, in the **System** page, click the **Summary** button to display System Summary, FRU data, and Power Supply as shown in Figure 2.



System Summary

Property	Value
System Name	linux-4aa2
Asset Tag	S3420GPC
BIOS Version	S3420GP.86B.01.00.0040
System GUID	843DC422565D11DE8B20001517980FFC
Manufacturer	Intel Corporation
Platform ID	S3420GPC
SDR Version	SDR Package 0.17
BMC Version	1.19
Serial Number	4444
Operating System Name	SUSE Linux Enterprise Server 11 (i586)
Operating System / Kernel Version	#1 SMP 2009-02-28 04:40:21 +0100
Operating System Build	2.6.27.19-5-pae

FRU Data

Device Name	Model Number	ID	Manufacturer	Part Number	Serial	Version
Baseboard	S3420GP	0	Intel Corporation	3333	4444	.....

Power Supply

Health	Name	Current Reading (Watts)	Upper Critical (Watts)

Figure 2. System Summary page

- Asset Tag: Name given to a server for easy server asset tracking such as hardware and software configuration information during server deployment.
- BIOS and Firmware version details. Current values obtained from server.
- System GUID value. Global Unique Identifier for each system on the network.
- IPMI version. Details of Intelligent Platform Management Interface version.
- SDR (Sensor Data Recorded) Package version, serial number of the server, and HSC version.

For systems that do not have compatible power supply, this page will not have instances. If the platform does not support power gauge sensors or PMBUS power supplies, then the current reading will be 0s (for example, H800t).

3.1.3 Viewing Processor Summary Readings

To view the processor summary readings, click **System** -> **Processor** to display processor summary, processor configuration, and discrete sensor readings shown as follows:

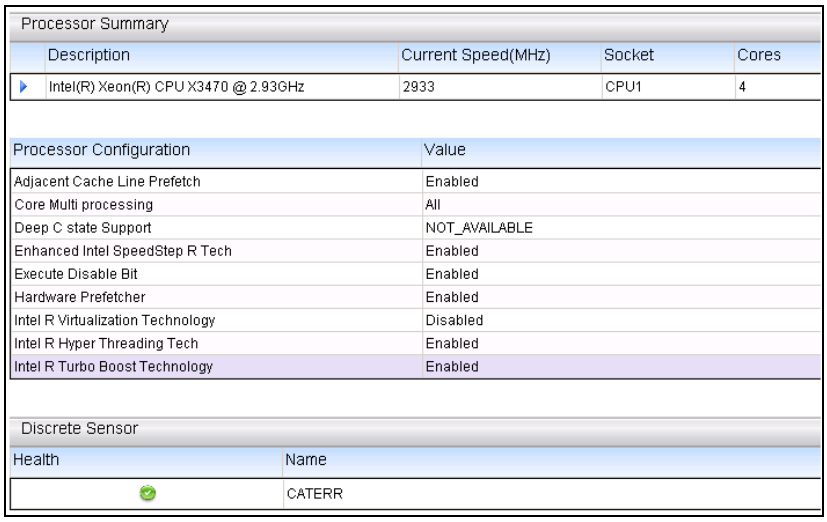


Figure 3 – Processor Summary Readings

As all thresholds are not supported for all sensors, unsupported thresholds are marked with a hyphen. Health of the sensors is also shown to indicate those that are critical and that are not.

3.1.4 Viewing Memory Device Readings

To view the processor memory device readings, click **System** -> **Memory** to display memory device details and discrete sensor readings shown as follows:

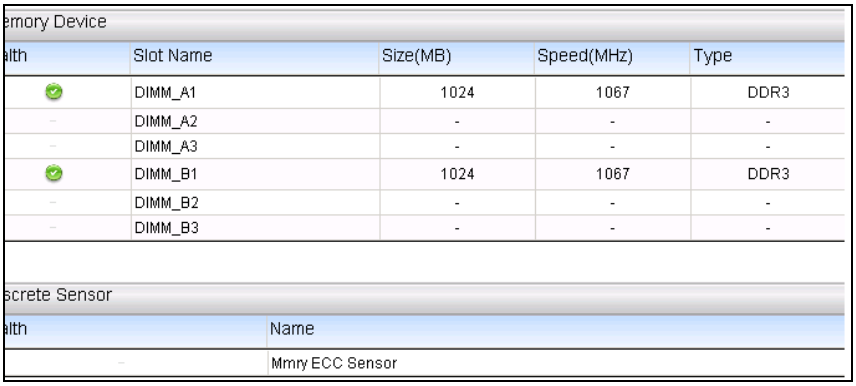
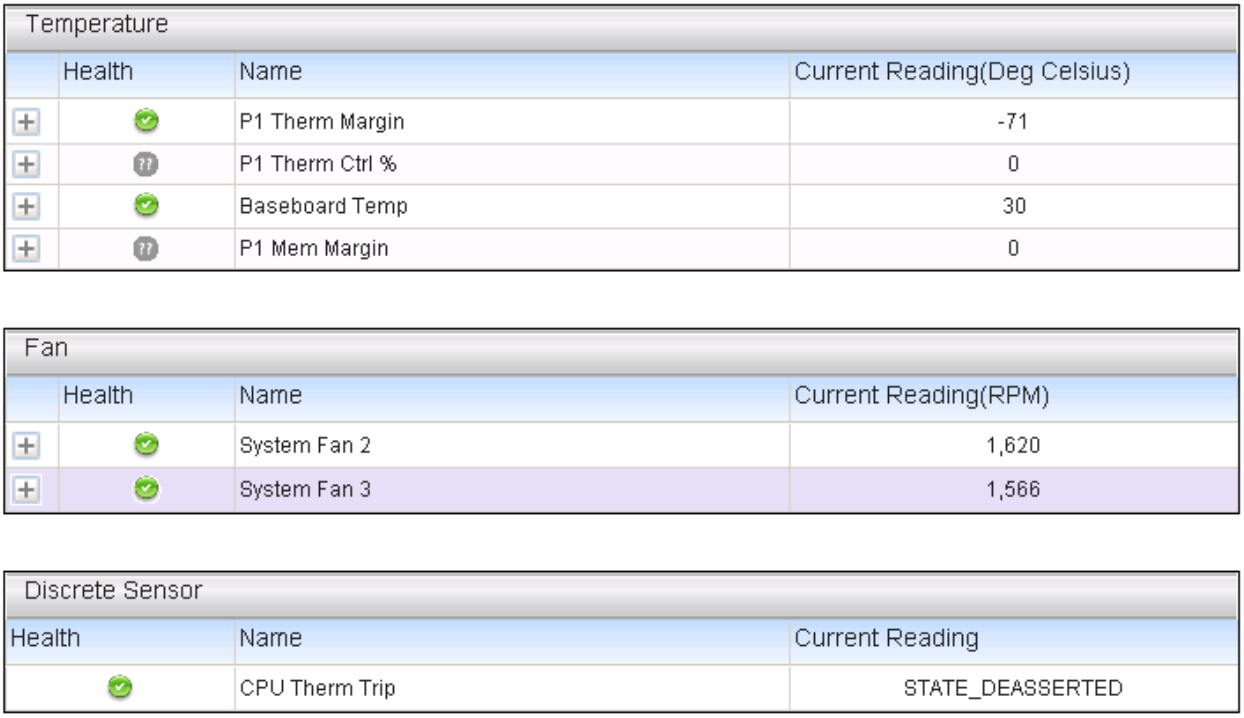


Figure 4 – Memory Device Readings

Displays the health of each of the populated memory module. It lists the entire memory bank supported in the Server. If a memory module is populated in the memory slot, it will list the corresponding size, speed, and type of module. If the slot is not populated, then it will list as not populated.

3.1.5 Viewing Temperature and Fan Readings (Cooling Sensors)

To view the temperature and fan readings, click **System** -> **Cooling** to display the Cooling Sensors page shown as follows:



Temperature

Health	Name	Current Reading(Deg Celsius)
✓	P1 Therm Margin	-71
?	P1 Therm Ctrl %	0
✓	Baseboard Temp	30
?	P1 Mem Margin	0

Fan

Health	Name	Current Reading(RPM)
✓	System Fan 2	1,620
✓	System Fan 3	1,566

Discrete Sensor

Health	Name	Current Reading
✓	CPU Therm Trip	STATE_DEASSERTED

Figure 5 - Cooling Sensors

Displays all System/Processor fans. It shows the current health status of the fan and the current reading of the fan in RPM. Click on any of the System/Processor fan to view the upper and lower threshold details.

3.1.6 Viewing Voltage and Current Sensors Readings

To view the temperature and fan readings, click **System** -> **Power** to display the Voltage and Current Sensors page shown as follows:

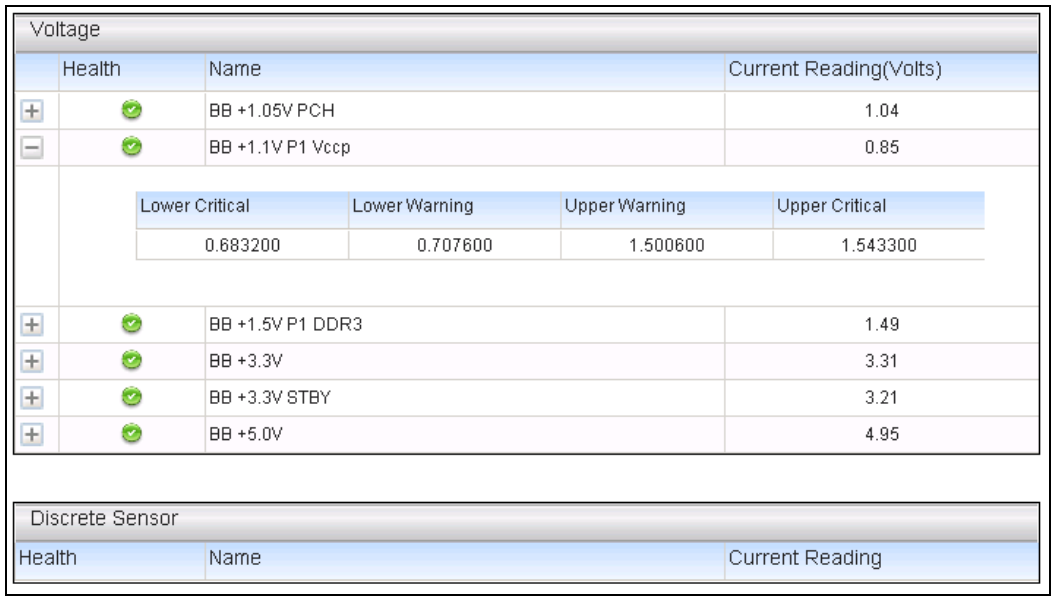


Figure 6. Voltage Sensors

Lists all the current reading of the voltage sensors present on the base board. The details of each voltage sensor list the upper/lower critical and warning values.

3.1.7 Viewing Chassis Information

To view the temperature and fan readings, click **System** -> **Chassis** to display the Chassis Sensors page as shown in following figure. The user can also identify the server by turning the LED on or off. To do this, click the chassis icon in this screen.

Notes:

- For systems that do not support the chassis sensor, **The system LED is currently Not Supported status** displays.
- For some platforms, the status of LED is not supported, but the user will still be able to turn the LED on and off as shown in Figure 7. To do this, click the chassis icon in this screen.

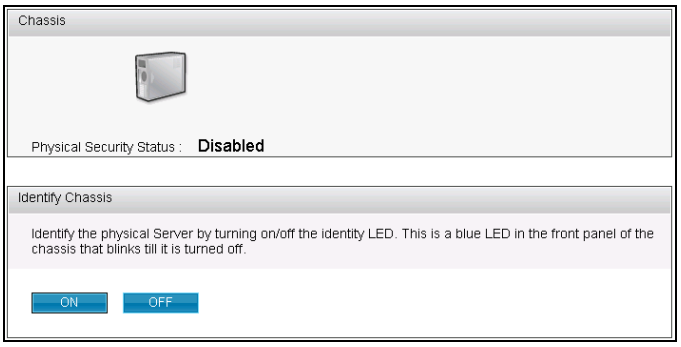

Chassis
Physical Security Status : Disabled
Identify Chassis
Identify the physical Server by turning on/off the identity LED. This is a blue LED in the front panel of the chassis that blinks till it is turned off.
ON
OFF

Figure 7 – Chassis Information page/ Identify Chassis On/Off Dialog

Displays physical security status of the chassis. Also helps identify chassis (physical Server) by turning the blue LED in the front panel of the chassis on/off (LED blinks till it is turned off).

3.1.8 Viewing Storage Readings

To view the temperature and fan readings, click **System** -> **Storage** to display the Storage Sensors page as shown in following figure.

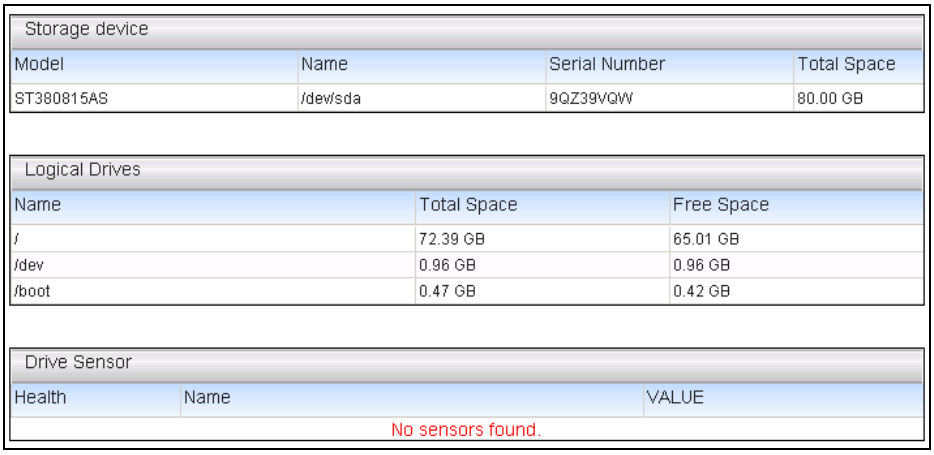


Figure 8 – Storage Device, Logical Drives, Drive Sensor Information page

- **Storage Device**. The Storage page lists out all the Storage drives present in the server. The drive name along with the Model Number, device name serial number and the total capacity of the Hard disk.

- **Logical Drive**. The Logical drive shows all the Logical drives that have been mounted currently. It shows the total used space and the free space for each of the logical drive.

- **Drive Sensor**. The Drive sensor displays two types of sensors basically the Drive Status and the Drive Presence sensors. It gives the name of the drive slot, the corresponding health of the Hard drive presence or absence.

  A warning alert gets generated in the Events page if the Hard disk space crosses the threshold of 75% and a Critical alert is generated if it crosses the 905 margin.

3.1.9 Viewing Miscellaneous Readings

This section lists out all the Sensors which are not categorized under any of the main pages. These include some BIOS and other discrete sensors. It lists the name of the Bus Sensors and shows the corresponding health along with the values.

Figure 9. Miscellaneous Information page (Bus Sensors, BIOS and other discrete sensors)

3.1.10 Viewing System Events

This page lists all the server events as follows:

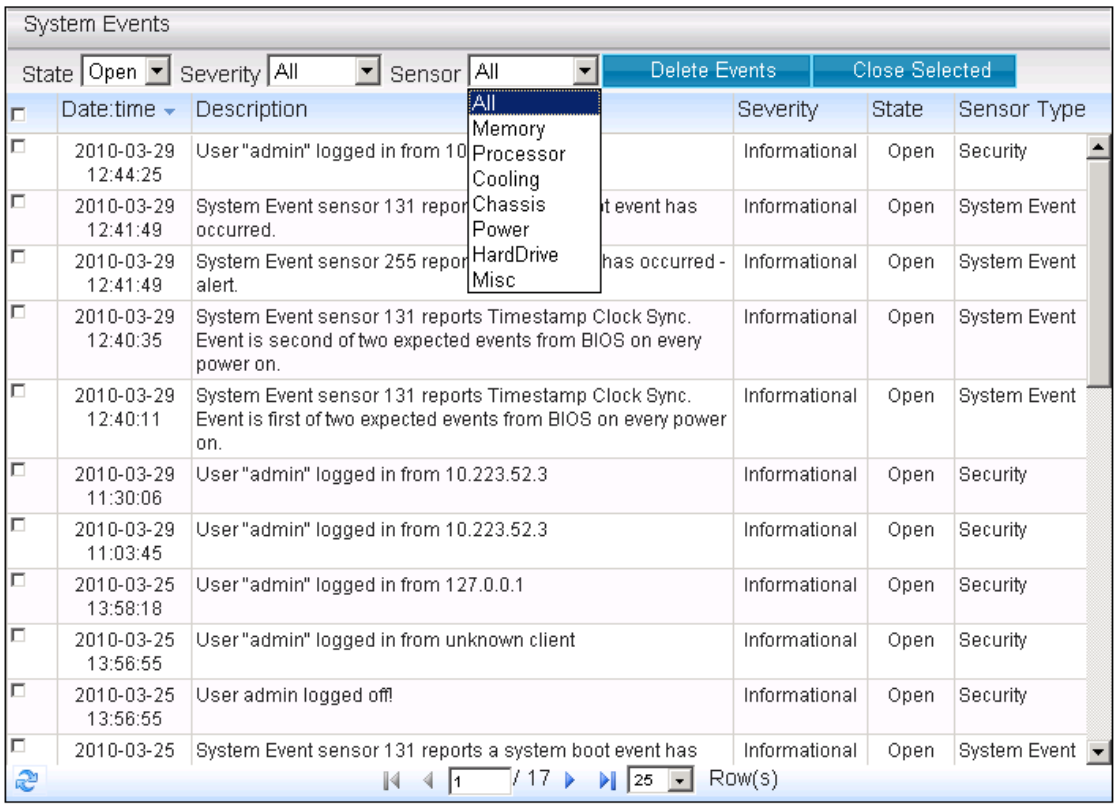


Figure 10 – System Events Information page

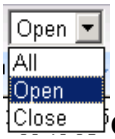
The description, severity, status of events (open or closed) and time stamp for each of the events is listed.

The top row heading shows a list of filters and actions that can be taken on the table. There are filters for State, Severity and Module Type. If a particular value in filter is selected, only events belonging to that filter value appears in the table.

-

Severity filter. Use for viewing only critical/warning/informational events. The column headings follow the filters and actions. The entire table can be sorted based on each column.

  To sort the table based on a column click on column heading. First click on the column sorts it in ascending (lexicographic) order. Any further clicks, the order toggles between ascending and descending.

- 

Open Status. If in open state, check for event description. If critical event, take immediate corrective action.

Actions

Two sets of actions can be performed on events.

- **Delete Events**. All the events listed in the table can be deleted from database. Here again, two options are available:

  Delete all events from Database. Here the events are deleted from ASC database. This include all open and closed Server Events as well as Application Events.

  Delete all events from Baseboard Management Controller (BMC). Here the Server Events are deleted from BMC SEL store.

  Notes:

  You cannot selectively delete events from either database or BMC. Either all events or none are deleted.

  If you delete from database, it cannot be recovered. So, backup event logs by exporting Reports.

- **Close Selected**. Update the status of events to closed. Based on the type of events two results are observed. If the event is regular events, close will just update the status to closed. If any active events are appearing in bottom scroll log, that will be gone. If the event contributes to Server health, displayed as ”Open *” in the Status column, closing the event causes the IASC to ignore the event and recompute the health of the component. This may cause the health of the Server from being critical to go to healthy state in IASC (if the event that closed is the only one causing the critical state).

  For instance ”memory ….”

- **Export tab**. Use for exporting log files in XML, CSV, or HTML format.

4 Configuring Server Hardware and Reports Generation

This section explains configuring the server hardware using IASC. It details the options available in the Configuration feature of the Intel® Active System Console. Click **Configuration** button to access the menu with the configuration options on Baseboard Management Controller as follows:

***Note*:** *Only users with ADMIN privilege can configure a Server using ASC*.

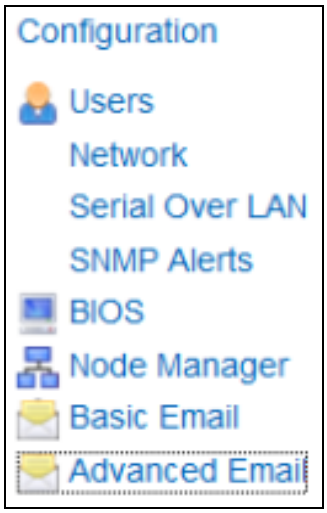


Figure 11 – Configuration Menu

4.1 Configuring BMC

This section explains configuring the BMC. It details the options available in the BMC Configuration feature of the Intel® Active System Console. The BMC Configuration window has the choices listed in Figure 11.

4.1.1 Configuring BMC Users

The BMC User Configuration section helps you edit a BMC User. While doing so, you can set the privilege level as Administrator, Operator, or User.

Baseboard Management Controller supports authentication and authorization for remote access(out-of-band access). Users have to configure a BMC Username and password to access BMC in out-of-band fashion

You can also enable or disable the User.

In the left navigation pane, click the **Configuration>BMC>Users** button to view the BMC User window as shown in Figure 12.

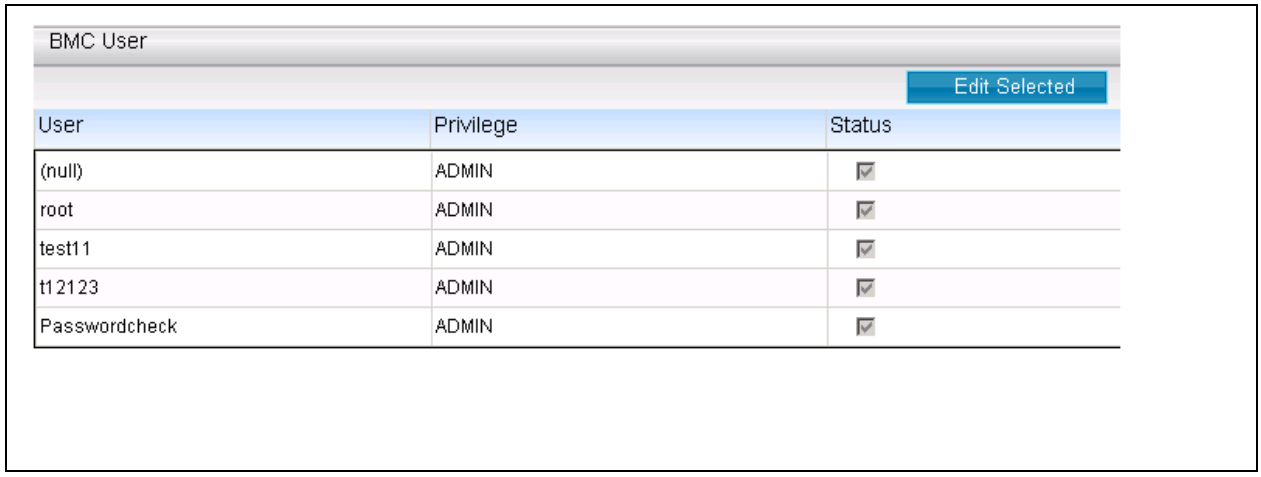


Figure 12. Intel ® Active System Console BMC User Configuration window

You can enable or disable the User by clicking **Edit Selected** to display the following dialog:

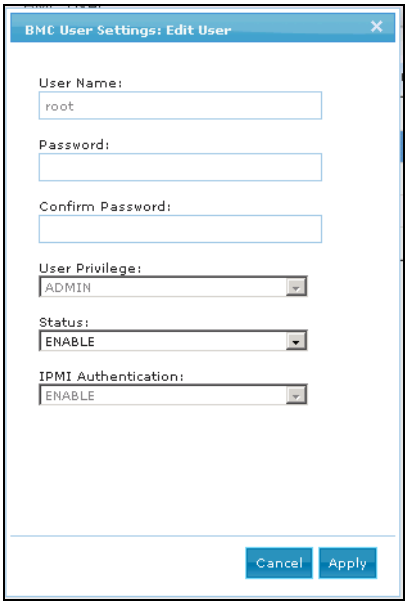


Figure 13. Configuring BMC User Settings: Edit User dialog

4.1.2 Configuring Network

Click Configuration>BMC>Network.

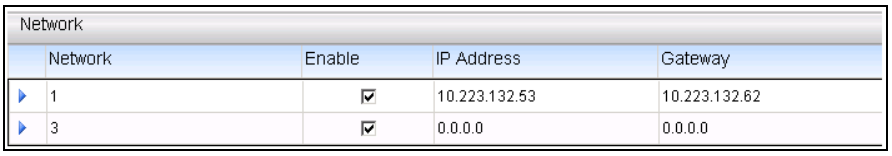


Figure 14. Configuring BMC Network Window

This page lists all the networks present on the motherboard. This indicates the LAN channels over which a baseboard controller (BMC) can be reached out-of-band.

To enable, check the enable box.

- To edit the settings, select the network channel and then choose either static or DHCP IP address.
- If you are choosing the option ”IP address from a DHCP server” then you must have a DHCP Server present in your network environment for the server to obtain an IP address automatically.
    - User Privilege can be either set to Admin, User, or Operator.
    - Admin user privilege configuration is needed for read, execute, and write privileges.

***Note**: These are not Operating System IP Addresses.*

4.1.2.1 LAN Failover

BMC FW provides the LAN Failover capability such that the failure of the system HW associated with one LAN link will result in traffic being routed to an alternate link.

Intel ® Active System Console enables LAN FAILOVER feature dynamically on the supported platform. On enabling LAN FAILOVER, only LAN Channel No. 1 will be allowed for configuration. Other active LAN channel share the same configuration when the network connection of LAN channel 1 is broken.

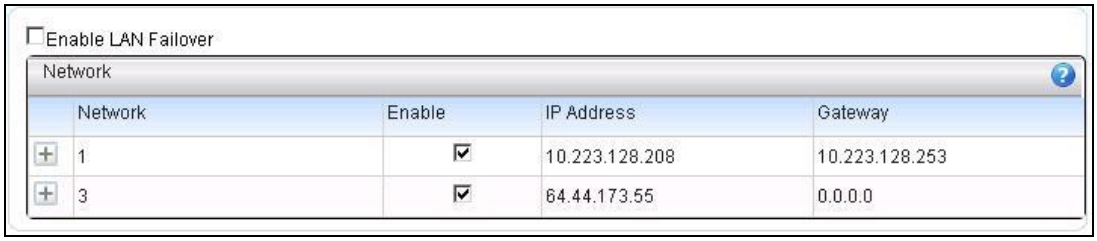


Figure 155. Configuring LAN FAIL Over

Note:

This feature is supported only on Intel® Xeon® Process X5 family based platforms. For more details on LAN Failover feature, refer Motherboard TPS.

4.1.3 Configuring Serial Over Lan (SOL) Settings

Base-board controller supports re-direction of Server boot sequence video console over LAN channel. Users can see the entire screen output of boot sequence and control it using keyboard simulating actual Server control. This console is lost once the operating system boots up. This feature is known as Serial-over-LAN.

Using ASC you can enable/disable or edit Serial-Over-LAN settings in base-board controller.

To change SOL settings, select LAN channel -> select baud rate -> select privilege level -> click **Update**.

You can enable authentication in which case only users with valid username and password can do SOL console redirection.

You can enable encryption in which case the entire SOL traffic will be encrypted and protected from network snooping.

Click **Configuration>BMC>Serial Over Lan** to display the **Serial Over Lan** window as shown in following figure:

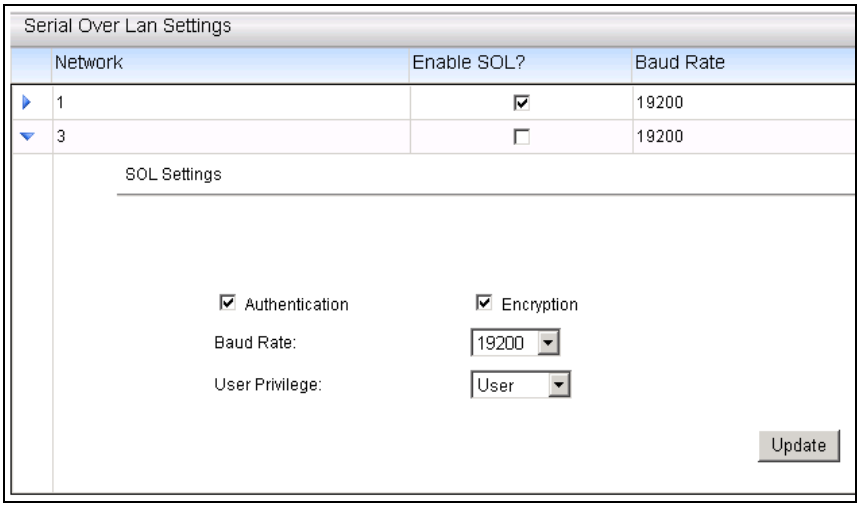


Figure16. Configuring SOL Settings Window

Note:

Configuring Baud Rate will not be supported on Intel® Xeon® Process X5 family based platforms. For more details, refer Motherboard TPS.

4.1.4 Configuring SNMP Alerts

SNMP Alerts help send SNMP -based alerts to the target server. Alerts include fan failure, memory error, and so on.

If you want base-board controller to send alerts about any change in Server hardware in the form of SNMP Traps to any SNMP Manager you can set it up using Active System Console.

SNMP Alerts help send SNMP Traps to the target server. Alerts include fan failure, memory error, and so on. Click **Configuration>BMC>SNMP Alerts** to display the SNMP Alerts settings window as shown in following figure:

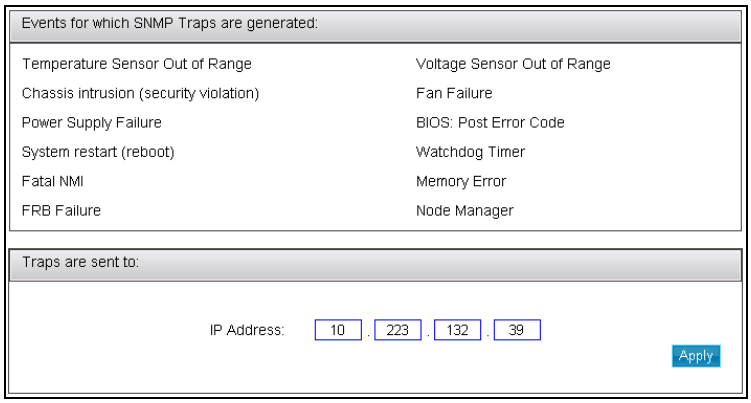


Figure17. Configuring SNMP Alerts Settings Window

To set an alert, enter the IP address of target SNMP Manager or trap receiver-> select the alert type from the list of alerts -> click **Apply**.

4.1.5 Configuring BIOS

Click **Configuration>BMC>BIOS** to display the BIOS settings window as shown in the following figure:

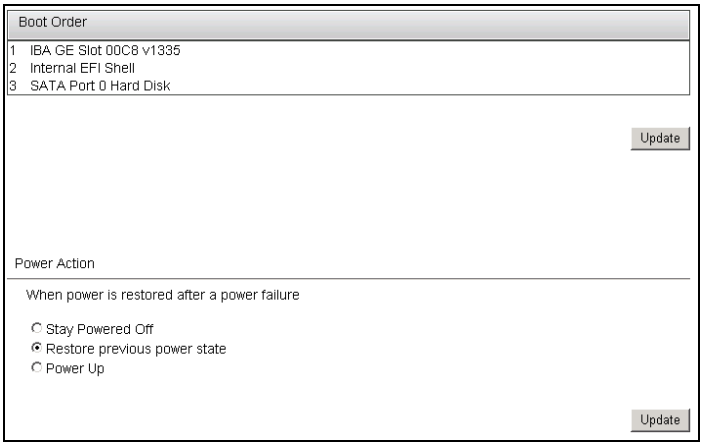


Figure 18. Configuring BIOS Window

Set Boot Order. Helps select system boot order - Hard Disk, DVD, Network, and so on - for the next reboot cycle. Select desired boot order -> click **Update**.

When Admin Password is set on the BIOS, user will be prompted as shown in the below image to enter the BIOS Admin password to update the boot order change. This feature is supported only on Romley.

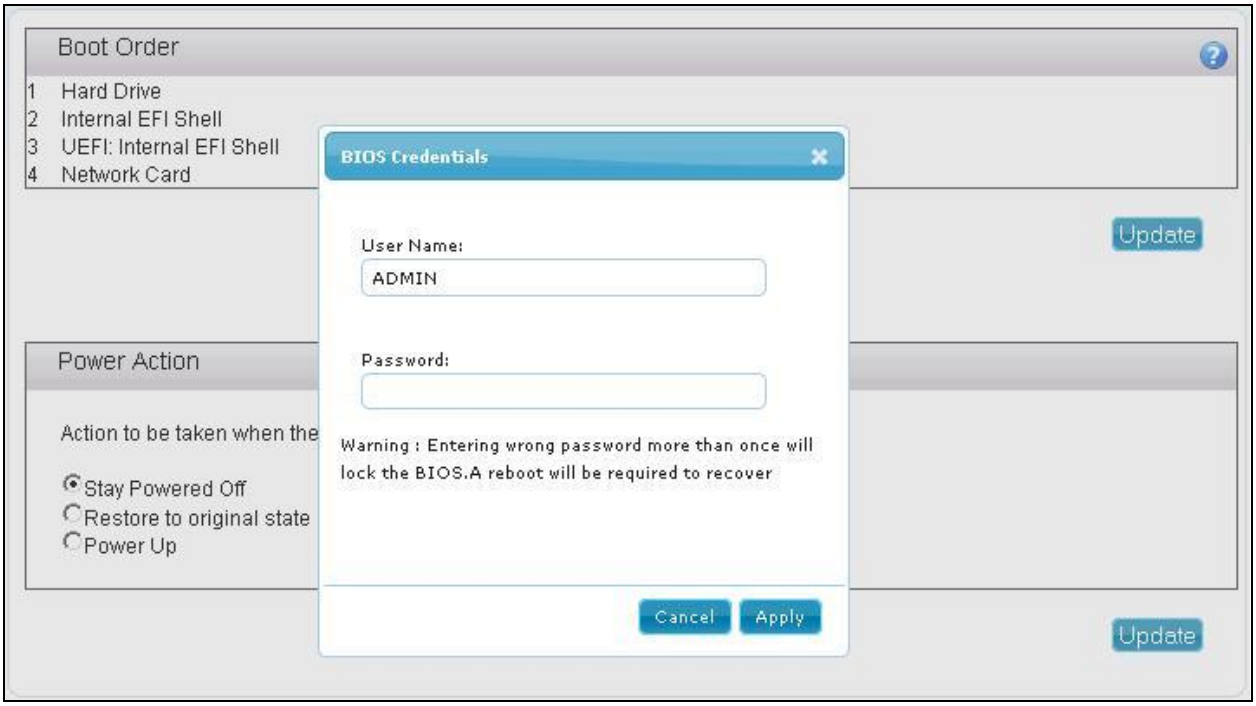


Figure 169. BIOS Admin Credentials for Boot Order

Power Action. Helps set power action in case of power breakdown. You have the option to choose one of the following:

- Stay powered off. Server remains in a powered off state even if the power is restored back.
- Restore to Original State. Server will either get powered up or it will remain in an Off state depending on previous power state during the power breakdown.
- Power Up. Server powers up when the power is restored back.

4.1.6 Configuring Intel® Dynamic Power Node Manager (Node Manager)

The Intel® Dynamic Power Node Manager (Node Manager) is an advanced system power savings feature to help user set power policies. Click **Configuration>BMC> Node Manager** to display the Node Manager Settings window as shown in following figure:

Figure 20. Configuring Intel® Dynamic Power Node Manager (Node Manager) Window

Power policy can be set for a specified power range only. Additionally, it can be applied for all/selected days. Refer to the *Intel® Dynamic Power Node Manager White Paper* for more details.

To create/edit a power policy setting, follow these steps:

1. Find and note current power reading of the server.
2. Find the average power consumed by the server during the day.
3. Select **Add** to add a new power policy or select one policy and click **Edit**.
4. In the profile window, enter a power limit value which is 25% higher than the average power consumption of the server. For example, if power consumption on an average is 140W and the peak power consumption is 210W then, enter a value for power limit as 170/180 Watts. NOTE: This is only an example and the power limit will vary depending on the server configuration. Refer the *Intel® Dynamic Power Node Manager White Paper* for limitations.
5. After entering power value, enter start and end time for power policy.
6. Select the recurrence days for the power policy. Either all days (daily) or specific a day (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday) can be selected.
7. Check the Alerts box if you also need alerts for the Intel® Dynamic Node Manager power policies.
8. After completing steps 1-7, click **Apply** to apply the settings.

   The Node Manager main page has an option for enabling/disabling the Node Manager policies. The user can enable all the policies or choose selected policies.

   If there are two policies overlapping a specific time, then the policy in which the power limit is low is the power policy that will be effective for that time period.
9. To delete a Node Manager Policy, select the policy using the check box and click **Delete policy**.

4.1.7 Configuring Basic Email: Use Default Email Profile

Email Alerting helps you receive Server Health Alert messages. For this, you must first configure your mail settings either through Basic Email settings or through Advanced Email settings.

Click **Configuration>Basic Email** to display the Email Alerts Settings window as shown in following figure:

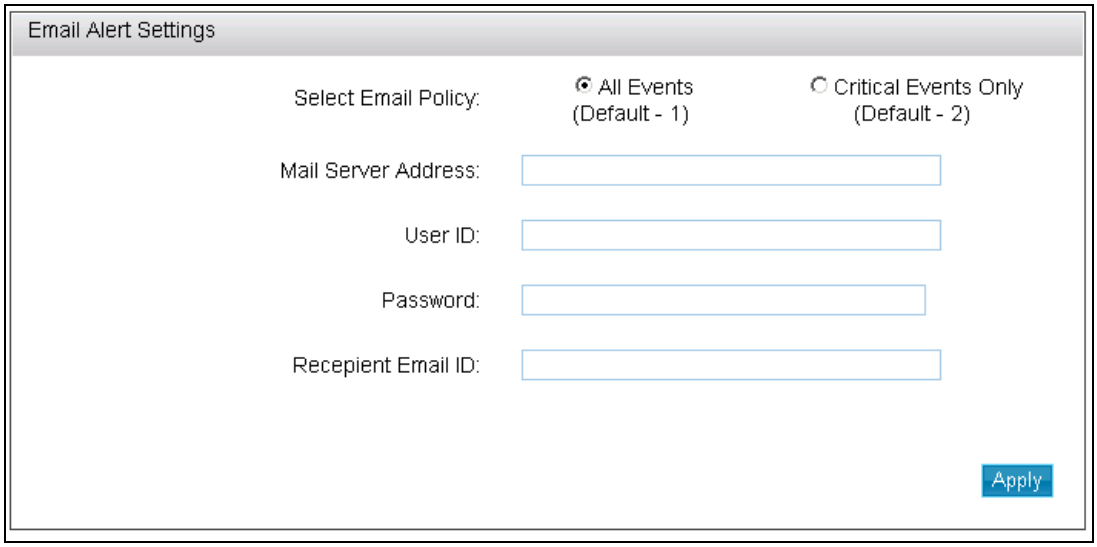


Figure 21. Basic Email Alerts Settings Window

Email Alerting helps you receive Server Health Alert messages. For this, you must first configure your mail settings either through Basic Email page or through Advanced Email.

For configuring Basic Email settings, you must have a mail server in your network environment. If not present, you must setup a mail server to use this feature.

- Select Default -1 profile to receive all Hardware alerts that include critical, warning, and informational.

OR

- Select Default-2 profile to get only the critical Hardware events alert.

Enter the mail server IP address, its hostname and then enter the **To** Email address to which the alert has to be sent. Click **Apply** to set the basic Email alert setting.

4.1.8 Configuring Advanced Email: Create and Apply Email Profiles

Click **Configuration>Advanced Email** to display the advanced **Email Alerts Settings** window as shown in following figure:

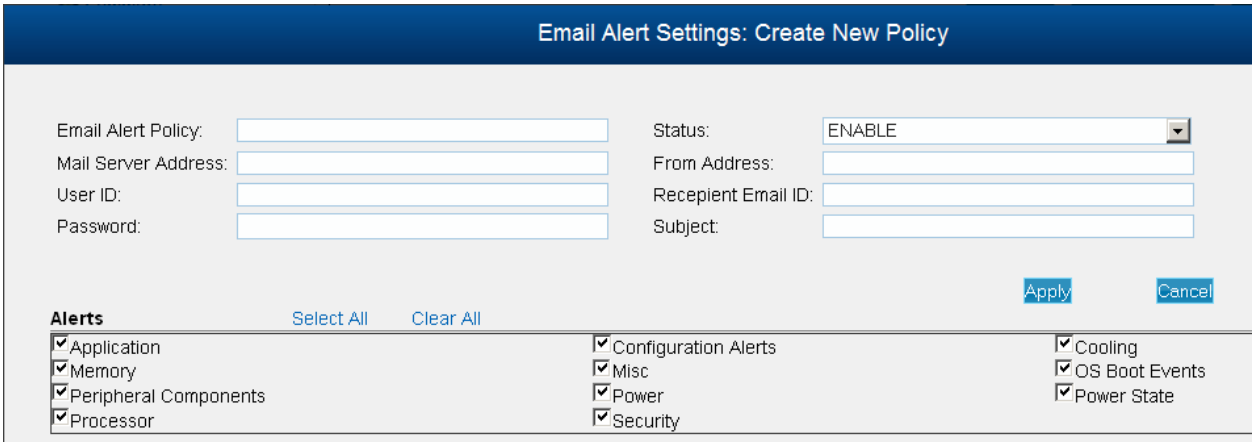


Figure 22. Advanced Email Alerts Settings Window

Advanced Email Settings is rich in customized user settings. To create an advanced Email, do the following:

1. Enter the following:
    - Profile name
    - Mail server IP address. If a mail server is not present, then you need to set one up to use this feature.
    - From address of the Email
    - One/multiple ”To” address/s
    - Subject line. For example, Chassis Intrusion Detected
    - Specific comments
2. Next, in the Alerts pane
    - Click **Select** all to select all the alerts (Select **Clear All** to deselect all as needed)

    OR

    - Select only specific alerts based on your need.
3. Next, click **Apply** to apply the settings.

To create another advanced Email, create a separate profile in step1 and then follow the same procedure.

4.2 Generating Reports

This option helps you generate reports on categories such as Asset Information, All System Events, Critical Events, Sensor Values, and BMC Settings. Click **Reports>Generation** to display the **Report Generation** window as shown in following figure:

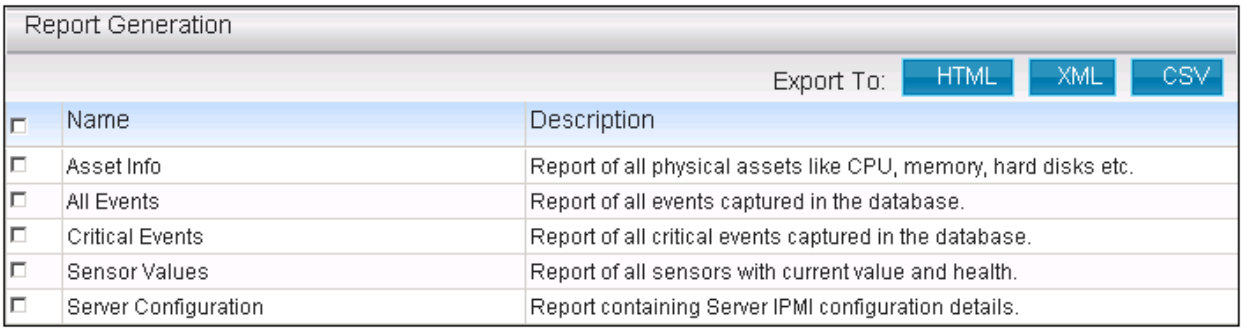


Figure 23. Generating Reports Window

The file can be exported either in HTML, XML, or CSV format.

4.3 User Settings

A User setting icon is provided on the main IASC page on the top corner right hand side.

Clicking on the setting icon will open the user setting page. Here, new users can be added or existing user privilege can be edited or users can be deleted.

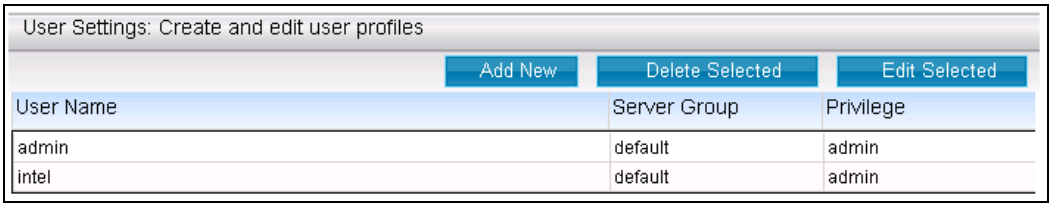


Figure 24. User Settings Window

***Note**: It is advised to give minimum number of administrator/root privileged users.*

4.4 Viewing Software Updates

The Active System Console periodically checks for new software updates for Active System Console, BIOS or firmware from Intel site. If there are any new updates applicable to the platform or operating system installed or any new product announcements, it shows up on the **Software Updates** link. The Software Updates page displays severity and description of the software update applicable and also a download link for downloading the package.

Click on Help drop-down menu and select **Check for Updates**, to view the page as follows:

Figure 25. Software Updates (system) window

You can initiate a download after deciding to install the package upgrade. The file thus downloaded can be installed per specific instructions given for a package.

The Check for Updates will work only if the Server is connected to a public network or if the OS can contact the public www.intel.com site without any configuration change. The Active System Console will not do any proxy settings by itself; it has to be configured by the user. If the agent is not able to contact Intel website, the update process does not show the new updates to the user.

You can choose to disable periodic Software Updates check by deselecting the check box for "Check periodically for software updates and new packages".

Once the option is selected, click on **Save Configuration** button to enable the selection.

5 Security Features

The Intel® Active System Console offers multiple security features as protection against unauthorized access to the application.

- It supports role-based multiple user authentication as follows:
  - ADMIN. Users with administrator privileges.
    Default Administrator user is admin. Only admin can create new users and assign privileges. Any user can, however, change password.
  - USER. Users with read-only privileges. Configuration changes using the application not permitted.
- IASC supports SSL based data encryption to securely communicate between client and application
- Secure Socket Layer allows two communicating devices to encrypt data using a public certificate and private key.
- The certificate used in IASC is a self-signed one to reduce the cost of deployment. All modern browsers will detect self-signed certificate and give a warning that the "certificate is invalid" since the authority that signed the certificate is not a publicly acknowledged authority. However, Users can override the warning and accept the certificate. You should do this only if you are sure that the certificate is originated from the application itself (by making sure you first launch the application from a trusted network and add the certificate to the trusted list).

  Once a certificate is accepted, the warning goes away as long as you launch the application from the same client.

  Customers having a valid certificate from a public CA can use that certificate instead of auto-generated one.

Replacing Certificate in a Windows* Installation

To replace certificate in a Windows* installation, do the following:

1. After installation, shut down the web-server for Certificate replacement.
   - Run services.msc from Run command in Windows. This will launch Services window.
   - Search for LightTPDService and stop the service.
2. Go to application installation directory (C:\Program Files\Intel\ASC\ in default case) and go inside conf folder.
3. Replace lighttp.crt with your valid certificate. If the name is different rename it to lighttp.crt.
4. Replace the private key file, lighttp.pem with your private key file.
5. Set all the permissions of the key file to only Administrator. No other users should be able to read or write this file.
6. Set the permissions of the lighttp.pem to read-write for Administrator and read-only for other users.
7. If you do not want to change the file names of your certificate/key file pair, make appropriate changes in the lighttpd-inc.conf in the same folder.
8. Restart the web-service LightTPDService from the Service window.

Replacing Certificate in Linux* Installation

To replace certificate in a Linux installation, do the following:

1. After installation, shut down the web-server for Certificate replacement. /etc/init.d/lighttpd stop.
2. Go to the folder /etc/lighttpd/ and replace lighttp.crt with your valid certificate. If the name is different rename it to lighttp.crt.
3. Replace the private key file, lighttp.pem with your private key file.
4. Set the permissions of the files as below:
   -rw-r--r-- 1 root root 1326 Mar 28 12:11 lighttp.crt
   -rw------- 1 root root 3005 Mar 28 12:11 lighttp.pem

   Only root is allowed to read the private key file and write the public certificate file
5. If you do not want to change the file names of your certificate/key file pair, make appropriate changes in the lighttpd.conf in the same folder.
6. Restart the web-server
   /etc/init.d/lighttpd start

- IASC uses a custom http TCP port (9393) so it does not conflict with site's access control lists or firewall rules
  For proper access to the application, appropriate changes should be done in firewall rules to exclude this port from blocking.
  Customers can modify the port if they want by editing the /etc/lighttpd/lighttpd.conf (in Windows, %ProgramFiles%\Intel\ASC\conf\lighttpd-inc.conf) and restarting the web-service.

- IASC uses TCP port 7777 for the communication between IASC and Intel® Multi-Server Manager (MSM). The port can be blocked by customer firewall if you don't have MSM.

- IASC may use TCP port 9191, 4369, 521 for internal only, those ports all can be blocked by firewall for security purpose.

Traceability and Security Audit

- IASC keeps track of who all logged-in and logged out and from which client. Any unauthorized attempts to login are also kept track of. This is recorded in the form of events in the Event Table.

Administrators of the tool should periodically do an audit on the events table to find out if there is any misuse of the application or any unauthorized attempts to access the tool.

5.1 Security Recommendations

No security feature is fool proof unless you follow certain standard security procedures and controls.

- **Security controls**. Implement, update and monitor industry security products for servers, such as but not limited to: anti-virus, anti-spyware, host based firewall, intrusion prevention, and so on.
- **Remote access.** The platform should be managed by those familiar with securing remote access functions as well as managing systems that are exposed to the Internet.
- When assigning passwords for the ASC and BMC user accounts, make them strong enough to minimize your risk that someone could guess the passwords and thus use the ASC to change the server configuration or interrupt its power/temperature controls. ASC warns the user if the password is weak, so follow the warning and guide-lines.
- **Network controls.** If the management console is being established to allow internet based access it is recommended to be placed within a network enclave that is consistent with many companies' internal policy of maintaining a "DMZ" or zone of networks that is more closely monitored than internal networks
- **Firewall**. Enable firewall software/services on Server where you install ASC or to the network, and only enable exceptions to allow access to the web server on each server. Where possible, limit which remote clients (e.g. using IP address ranges) can connect to the web server.
- To prevent successful Cross-Site Scripting and Forgery attack (XSS/CSRF) the users should follow certain security guidelines:
    - Make sure you access the application only from trusted clients.
    - Do not leave the application logged-in for a prolonged time and close the browser as soon as you finish the usage.
    - Do not visit any suspicious site or click on any public links in any other tabs in the browser while you are accessing the application.
    - Change the passwords frequently to prevent unauthorized access by any internal user and to reduce social engineering attacks.
    - Delete and create new application user accounts to reduce the risk of unauthorized access from internal users or ex-users.

6 Troubleshooting Guidelines

If you face any issues or doubts while using IASC, you can refer to the Help available in each page of IASC.

If the issue persists, read the following sections for troubleshooting tips and known issues.

Troubleshooting Tips

1. If, even after giving correct username and password, you are not able to login

   OR

2. You logged in and while using the IASC, it does not respond.

   The issue could be that any of the previous requests is taking too much time to respond to or the Base-board Management Controller interface has become unresponsive. The best way to resolve is to restart the essential services of IASC.
   For this do the following steps:

   In Windows*,

   - Run the batch file "IASCService.bat" in the Installed path or do the steps manuallygo to Start menu, and click on Run (Windows 2003, XP)
   - go to Start menu, and click on *"Search programs and files"* box
   - type *services.msc* in the box and press <Enter> key. The Services window will come up.
   - Search for IASCServiceManager service and stop the service
   - Search for "Appcore" service and stop the service.
   - Start "Appcore" service and IASCServiceManager one after another.

   In Linux*,

   Run /usr/local/asc/bin/IASCService.sh or

   - Open a terminal window and run the following commands
   - /etc/init.d/lighttpd stop
   - /etc/init.d/ascpolicy stop
   - /etc/init.d/Appcore stop
   - /etc/init.d/Appcore start
   - /etc/init.d/ascpolicy start
   - /etc/init.d/lighttpd start.

   This will solve most of the unresponsive situations. You can launch the browser and

login to the tool again.

3. If you are not able to access IASC installed in a Server from a remote location but able to ping the Server or connect remotely to Server, then it could be a firewall issue. Troubleshoot this by disabling firewall temporarily and try connecting to the IASC URL remotely again. If it works, then try adding following ports to the exception list of firewalls to the Server.

   Active System Console uses few ports (9393, 9191, 7777) which should be excluded from firewall if you have to reach the tool from other systems or from outside the private network.

4. If at any time, any of the following essential services of IASC are down, IASC will not work. If you are facing some issues in accessing the product, you should check if the following services are running.

   In Windows*,

   IASCServiceManager

   Appcore

   In Linux*,

   Run the following commands and verify

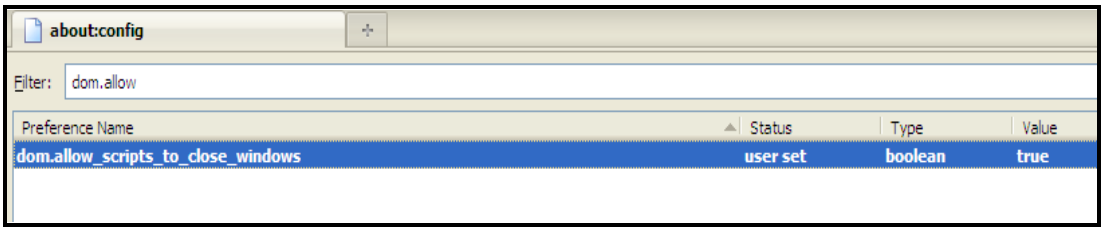
   /etc/init.d/lighttpd status

   /etc/init.d/ascpolicy status

   /etc/init.d/Appcore status

Known Issues

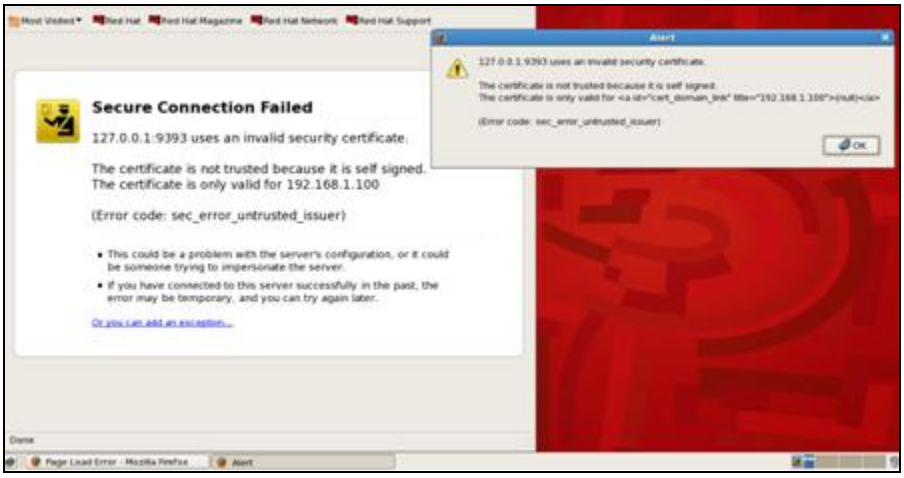
1. ASC needs several minutes to collect system data at first time running, it may show information “data is being retrieved, please retry”. This is normal; wait a moment and try to re-login ASC. If you always encounter this information after logging into ASC, you may need to check the hostname resolution on your server includes domain name server setting or hosts file configuration.
2. Parts of IASC pages, such as memory, processor, are not available on system that install on GPT style partition.
3. In Active System Console any event which has severity NOT_AVAILABLE (like PCIe Corr sensor event) will not be considered for health calculation.
4. Intel Active System Console install Microsoft Visual C++ 2005 Redistributable (x86) as a pre-requisite.
5. License page cannot be closed by clicking "Close" button on some Linux* systems.
   To resolve, do the following:
   a) Launch Mozilla Firefox* and type `about:config` in the URL window.
   b) Search for “ dom.allow_scripts_to_close_windows ”, double click it and set it to “true”



c) Disable it after installation.

6. This product supports secure transport using SSL/TLS. SSL/TLS uses a self-signed certificate because of which the browsers will show a message of"Untrusted Connection" warning.

The following are screen shoot of this warning on Microsoft Windows* and Linux* OS


Secure Connection Failed
127.0.0.1:9393 uses an invalid security certificate.
The certificate is not trusted because it is self signed.
The certificate is only valid for 192.168.1.100
(Error code: sec_error_untrusted_issuer)
OK

The certificate used in Intel® Active System Console is a self-signed one to reduce the cost of deployment. All modern browsers will detect self-signed certificate and give a warning that the "certificate is invalid" since the authority that signed the certificate is not a publicly acknowledged authority. However, Users can override the warning and accept the certificate. You should do this only if you are sure that the certificate is originated from the application itself (by making sure you first launch the application from a trusted network and add the certificate to the trusted list). Once a certificate is accepted, the warning goes away as long as you launch the application from the same client.

To add your own certificate, please refer the User Guide.

7. While installing Intel® Active System Console , a user can experience the dependency error for "libxslt.so" in Red Hat* Linux* Enterprise 5.x. To resolve dependency error, libxslt.*.i686.rpm needs to be installed.
8. When generating Reports using the product in Internet Explorer*, go to 'Tools' menu->'Internet Options'->'Advanced'->'Security' and uncheck "Do not save encrypted pages to disk". Otherwise generated reports will not be saved in the local disk.
9. Some security settings in Internet Explorer* 7 or8 may block some data/Popup message. User will have to modify the security settings to enable Intel ASC to function as expected.
10. If a CD/DVD is inserted into a CD/DVD drive, Active System Console will always show up the Storage System and drive as critical with 0 space left. Once CD is removed, it comes back to healthy stage. This issue will be resolved in future releases.

11. The wait icon and critical events scrolling at the Active System Console will not work if the browser does not allow animations. Enable animations in browser for proper usage; For example, in IE, go to Tools-> Internet Options->Advanced->Multi Media and check the "Play animations" option.
12. While installing Active System Console in SLES OSs, user may experience these warnings.

    Insserv: warning: script 'K01Appcore' missing LSB tags and overrides

    Insserv: warning: script 'S01Appcore' missing LSB tags and overrides

    User can safely ignore these warnings.
13. Installation in Red Hat* Enterprise Linux 6.x x64_86 and above version requires the following minimum version of the packages preinstalled in the system
    a. libxslt-1.1.26.2-2.el6.i686.rpm
    b. libstdc++-4.4.4-13.el6.i686.rpm
    c. compat-libstdc++-33-3.2.3-69-el6.i686.rpm
    d. ncurses-libs-5.7.3.20090208.el6.i686.rpm
    e. openssl098e-0.9.8e-17.el6.i686.rpm
    f. libcurl-7.19.7-16.el6.i686.rpm
    g. libgpg-error-1.7-3.el6.i686.rpm
    h. libxml2-2.7.6-1.el6.i686.rpm
    i. libgcrypt-14.5-3.el6.i686.rpm
14. The button clicks and drop down lists will not work if the scripting is disabled in Internet Explorer 8 and 9. To resolve this, go to Menu -> Tools -> Options -> Security -> Select Internet Zone -> Custom Level -> Scripting should be set to "Enabled".
15. Installation on Virtual Environment, Non BMC Server Boards, Non Supported Platforms are not supported.
16. FRU details containing &, * characters will not be available in ASC. Hence, these values will not be shown.
17. IASC does not show separate HSC FW version for Intel® Server S1200RP product family
18. SOL BAUD RATE Configuration is not available for Intel® Server S1200RP product family. Hence, the value will be shown as "NOT_AVAILABLE".
19. IASC sets the power policy ID start from No.2 instead of No.1 when configure Intel® Dynamic Power Node Manager (Node Manager) feature. This issue will be fixed in future release
20. Pop-up massage box may not work If running IASC in window explorer for "Node Manager" and "Advance Email" features. To resolve this, go to web browser, select Tools -> Internet options>Security then choose "Internet", select Custom Level -> look for "Scripting" and click Enable for active scripting. Save Changes and restart internet explorer again.